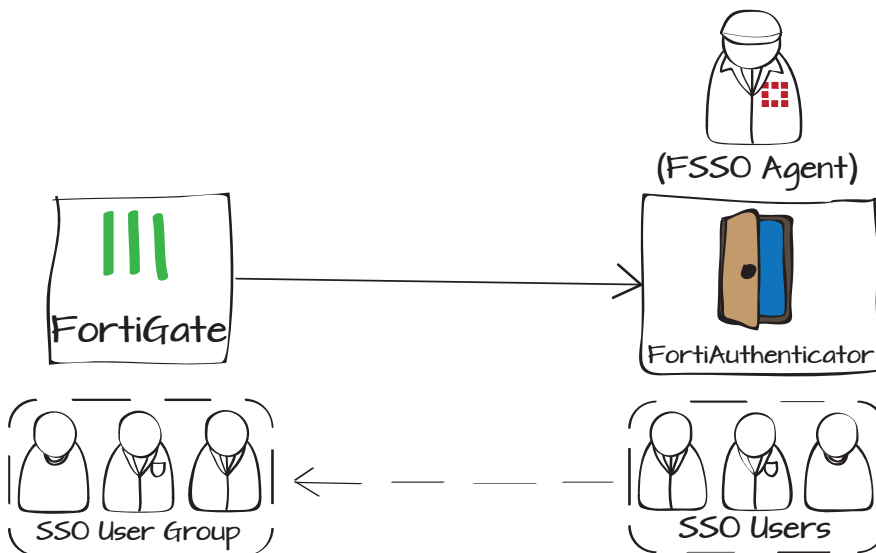


Allowing Single Sign-On access with a FortiGate and a FortiAuthenticator

This example illustrates how to configure Single Sign-On (SSO) using a FortiGate and FortiAuthenticator, with the FortiAuthenticator unit acting as the SSO Agent, verifying and maintaining user login information. Users can then log in once when connecting to the internal network behind the FortiGate, and be automatically logged into servers and services that support SSO.

1. Configuring polling on the FortiAuthenticator
2. Adding a FortiAuthenticator to the FortiGate unit
3. Creating the FSSO user group
4. Creating a security policy
5. Results



Configuring polling on the FortiAuthenticator

In the FortiAuthenticator interface, go to **SSO & Dynamic Policies > SSO > Options**.

In the **FortiGate** section, the Listening Port should be 8000, unless the FortiGate's default port mapping has been changed.

Select **Enable Authentication**, and enter the **Secret Key**, which you will use when configuring the FSSO Agent on the FortiGate.

If you are using an external SSO service, such as Windows AD or a remote LDAP server, enable it in the the **Fortinet Single Sign-On (FSSO)** section.

Go to **SSO & Dynamic Policies > SSO > Login Portal** and **Enable SSO Portal**. Ensure **Local users** is enabled, and disable **Remote users from an LDAP server**.

Then go to **SSO & Dynamic Policies > SSO > FortiGate Group Filtering**.

Create a new **FortiGate Group Filter**, entering the FortiGate's IP/hostname.

Enable **Forward FSSO information for users from the following subset of groups only** and move the groups you'd like to send to the FortiGate from **Available** to **Selected**. Select **OK** to save the filter.

The screenshot displays the FortiAuthenticator configuration interface. The top section is titled "FortiGate" and includes fields for "Listening port:" (8000), "Login expiry:" (480 minutes), a checked "Enable authentication" checkbox, and a "Secret key:" field with masked characters. Below this is the "Fortinet Single Sign-On (FSSO)" section, which has a "Log level:" dropdown set to "Info". It contains several unchecked checkboxes: "Enable Windows Active Directory domain controller polling", "Enable RADIUS Accounting SSO clients", "Enable FortiClient SSO Mobility Agent Service", and "Restrict auto-discovered domain controllers to configured domain controllers". A "Restart SSO service" button is located at the bottom of this section. The next section, "Enable SSO Portal", has a checked checkbox and a label "Enable SSO for the following sets of users:". It includes a checked "Local users" checkbox with radio button options for "All local users" (selected) and "Local users from selected groups only", and an unchecked "Remote users from an LDAP server:" checkbox with a "[Please Select]" dropdown. Below this is a form for "Fortinet Single Sign-On (FSSO)" with fields for "Name:" (FGT-100D_Lab), "FortiGate name/IP:" (192.168.1.99), and "Description:". The bottom section is titled "Fortinet Single Sign-On (FSSO)" and has a checked checkbox "Forward FSSO information for users from the following subset of groups only:". It features two list boxes: "Available sso groups" on the left and "Selected sso groups" on the right. The "Selected sso groups" list contains the entry "fssample_group".

FortiGate	
Listening port:	8000
Login expiry:	480 minutes
<input checked="" type="checkbox"/> Enable authentication	
Secret key:

Fortinet Single Sign-On (FSSO)	
Log level:	Info
<input type="checkbox"/> Enable Windows Active Directory domain controller polling	
<input type="checkbox"/> Enable RADIUS Accounting SSO clients	
<input type="checkbox"/> Enable FortiClient SSO Mobility Agent Service	
<input type="checkbox"/> Restrict auto-discovered domain controllers to configured domain controllers	
<button>Restart SSO service</button>	

☒ Enable SSO Portal

Enable SSO for the following sets of users:

- ☒ Local users
 - ☒ All local users
 - ☐ Local users from selected groups only
- ☐ Remote users from an LDAP server: [Please Select]

Fortinet Single Sign-On (FSSO)	
<input checked="" type="checkbox"/> Forward FSSO information for users from the following subset of groups only:	
Available sso groups	Selected sso groups
<input type="text"/>	Select your choice(s) and click +
	fssample_group

Adding a FortiAuthenticator to the FortiGate unit

In the FortiGate interface, go to **User & Device > Authentication > Single Sign-On**, and select **Create New**.

For the **Type**, select Fortinet Single Sign-On Agent. Enter a **Name** for the FortiAuthenticator unit.

Enter the IP address of the FortiAuthenticator as the **Primary Agent IP/Name**, and enter the secret key as the **Password**.

Select **Apply & Refresh**, and wait a minute for the FortiAuthenticator to connect to the FortiGate and download user group information.

Name	<input type="text" value="My_FAC"/>		
Primary Agent IP/Name	<input type="text" value="192.168.1.117"/>	Password	<input type="password" value="....."/>
Secondary Agent IP/Name	<input type="text"/>	Password	<input type="password"/>
LDAP Server	<input type="text" value="Click to set..."/>		
Users/Groups	<div><div>View Users/Groups</div><div>Edit Users/Groups</div></div> <div><input type="text" value="FSSO_SAMPLE_GROUP"/></div>		

Creating the FSSO user group

You cannot directly use the user groups imported from FortiAuthenticator in firewall policies, so you will need to create FortiGate user groups to represent the FortiAuthenticator groups. Go to **User & Device > User > User Groups**, and create a new FSSO user group.

The **Members** list will be populated with the FortiAuthenticator's user groups. Select the imported groups to add them to the FortiGate group's **Members** list.

Name	<input type="text" value="FSSO_users_group"/>		
Type	<div><input type="radio"/> Firewall <input checked="" type="radio"/> Fortinet Single Sign-On (FSSO) <input type="radio"/> Guest</div>		
Members	<div><div><input checked="" type="checkbox"/> FSSO_SAMPLE_GROUP</div><div>✕</div><div>+</div></div>		

Creating a security policy

Now, create a security policy to handle SSO user traffic, so it can be easily identified in logs and reports. Go to **Policy > Policy > Policy**, and create a new policy, setting the **Policy Subtype** to **User Identity**.

Multiple **Authentication Rules** can be created for different groups of SSO users that require different access and supervision.

Results

With the identity-based policy being the only policy connecting the internal network to the internet, users on the internal network will not be able to access the internet without authenticating.

To connect to the internet, users must navigate in a browser to the FortiAuthenticator's IP. Users will then log into the FortiAuthenticator as an admin would, but will only have access to their user account settings in the FAC interface.

Once the user has logged in, the FortiAuthenticator retains their user information for a time specified in the SSO Portal settings. They will have access to the internet, and to any other services or servers on the internal network configured to use SSO with the FortiAuthenticator.

Policy Type	<input checked="" type="radio"/> Firewall <input type="radio"/> VPN
Policy Subtype	<input type="radio"/> Address <input checked="" type="radio"/> User Identity <input type="radio"/> Device Identity
Incoming Interface	port1
Source Address	all
Outgoing Interface	wan1
<input checked="" type="checkbox"/> Enable NAT	
Destination Address	all
Group(s)	FSSO_users_group
User(s)	Click to add...
Schedule	always
Service	ALL
Action	ACCEPT

Login

Username: twwhite

Password:

Login

[Forgot my password](#)